Document Title	Requirements on Diagnostic
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	004
Document Classification	Auxiliary
Document Status	Final
Part of AUTOSAR Release	4.2.2

Document Change History

Release	Changed by	Change Description
4.2.2	AUTOSAR Release Management	• Clarification of bootloader interaction • Interfaces for DCM communication via PDU router • Rework of document structure
4.2.1	AUTOSAR Release Management	• Support of WWH-OBD (Major change) • Support of UDS service $38 (“RequestFileTransfer”), (Change) • Added new requirements for runtime errors and transient errors (Change) • Aging of events (Change)
4.1.3	AUTOSAR Release Management	• New requirement for processing a new request in DEM • New requirement for event management mechanisms in DEM
4.1.1	AUTOSAR Administration	• OBD-specific configuration capabilities in DCM and DEM • Event de-bouncing in DEM • Freeze Frame and Extended Data Record handling in DEM • Support of SAE J1939 • Link Requiriement with BSW Feature Document • Updating format of requirements according to TPS_StandardizationTemplate
4.0.3	AUTOSAR Administration	• Clarification of DET functionality • Formal Rework for Requirements Tracing
4.0.2	AUTOSAR Administration	• Clarification of DET functionality (remove BSW04088)
3.1.5	AUTOSAR Administration	• Document structure reworked and extended • Improvement of DEM behavior description • Introduce the approach for functional diagnostics of SW-Cs • Added requirements for further diagnostic modules (DLT/DET) • Legal disclaimer revised

Document Change History		
Release	**Changed by**	**Change Description**
3.1.1	AUTOSAR Administration	• Remove requirement BSW04062 • Added requirement SRS_Diag_04082 for OBDII support • Legal disclaimer revised
3.0.1	AUTOSAR Administration	• Document meta information extended • Small layout adaptations made
2.1.15	AUTOSAR Administration	• “Advice for users” revised • “Revision Information” added
2.1	AUTOSAR Administration	• Legal Disclaimer revised
2.0	AUTOSAR Administration	• Minor formal changes
1.0	AUTOSAR Administration	• Initial Release

Disclaimer

Advice for users

AUTOSAR specifications may contain exemplary items (exemplary reference models, "use cases", and/or references to exemplary technical solutions, devices, processes or software).

Any such exemplary items are contained in the specifications for illustration purposes only, and they themselves are not part of the AUTOSAR Standard. Neither their presence in such specifications, nor any later documentation of AUTOSAR conformance of products actually implementing such exemplary items, imply that intellectual property rights covering such exemplary items are licensed under the same rules as applicable to the AUTOSAR Standard.

Table of Contents

1 Scope of document

The goal of AUTOSAR WP Diagnostics and this document is to define to what extent elements of the diagnostic basic software have to be configurable and what preliminaries they shall comply with to meet the tailoring requirements. The handling of the legislated OBD and enhanced Diagnostics shall also be achieved.

As far as possible the set of diagnostic basic software elements should consist of already existing elements of modules of automotive software. Only in case of ‘good reasons’ valid elements of basic software should be part of the set.

If such the definition of these valid elements is not part of this work package. Nevertheless the information about basic software elements additionally required shall be given to related work groups.

Constraints

First scope for specification of requirements on basic software modules are systems which are not safety relevant. For implementation of the basic software modules in safety relevant systems, it shall be checked if additional requirements are necessary.

For this document we refer to ISO 15031-5. The equivalent SAEJ1979 is not mentioned explicitly but is covered accordingly.

2 Conventions to be used

- The representation of requirements in AUTOSAR documents follows the table specified in [3].

- In requirements, the following specific semantics are used

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted . Note that the requirement level of the document in which they are used modifies the force of these words.

- SHALL: This word means that the definition is an absolute requirement of the specification.
- SHALL NOT: This phrase means that the definition is an absolute prohibition of the specification.
- MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase „SHALL NOT“, means that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- MAY: This word, or the adjective „OPTIONAL“, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation, which does not include a particular option, MUST be prepared to interoperate with another implementation, which does include the option, though perhaps with reduced functionality. In the same vein an implementation, which does include a particular option, MUST be prepared to interoperate with another implementation, which does not include the option (except, of course, for the feature the option provides.)

3 Acronyms and abbreviations

Acronym:	***Description:***
External diagnostic tool	It is a device which is NOT permanently connected within the vehicle communication network. This device could be connected to the vehicle for various purposes, as e.g. • development • manufacturing • service (garage) Know devices are e.g. • a diagnostic tester • an OBD scan tool The external diagnostic tool is to be connected by a mechanic to gather information from “inside” the car.
Internal diagnostic tool	It is a device/ECU which could be connected permanently within the vehicle communication network. The purpose of this device/ECU could be a functionality as e.g. • advanced event tracking • advanced analysis’s for service mechanics. The behavior of the device/ECU could be the same as if it is an external diagnostic tool. The meaning of ´internal diagnostic tool´ is NOT that it is included in each ECU as an AUTOSAR SW-Component.
AUTOSAR application	A SW-application above the RTE which is using the API’s defined by DCM and DEM
Monitoring path	A monitoring path represents a diagnostic symptom and it is assigned to a unique event ID.
Event	In case of the use of the term Event a Diagnostic event is meant.
Diagnostic test results	De-bounced and qualified test result provided by a monitoring function.

4 Requirement Specification

4.1 Functional Requirements

4.1.1 [SRS_Diag_04010] The DEM module and DCM module shall ensure interaction in order to fulfill ISO 14229-1 and ISO 15031-5

⌈

Type:	Valid
Description:	If the DCM module shall respond diagnostic services of a tester/scan-tool (e.g. read DTC information), the DCM module shall use interfaces to collect the required data from the DEM module (e.g. setting the DTC status mask, get filtered DTCs and the corresponding event related data) and from SW-Cs (e.g. read current diagnostic values). The DEM module shall provide interfaces to process the storage of events and event related data.
Rationale:	ISO 14229-1 v.2013 and ISO 15031-5
Use Case:	Improved fault and event tracking, analysis for services, assembly line, OBD-SCAN-Tool
Dependencies:	--
Supporting Material:	ISO 14229-1 v.2013 ISO 15031-5

⌋(RS_BRF_02184, RS_BRF_01440)

4.1.2 [SRS_Diag_04082] The diagnostic modules DCM and DEM shall provide standardized interfaces to support OBD services as defined in ISO15031-5 and SAE J1979

⌈

Type:	Valid
Description:	The DCM and the DEM provide interface to support OBD services $01 to $0A to access Parameter Identifiers (PIDs), diagnostic test results and further OBDII specific data.
Rationale:	--
Use Case:	--
Dependencies:	Configuration
Supporting Material:	--

⌋(RS_BRF_02144, RS_BRF_01440)

4.1.3 [SRS_Diag_04065] The DEM and DCM shall be able to remove a specific event or event groups from the configured event memory

⌈

Type:	Valid
Description:	The DEM and DCM shall process the deletion of events or event groups according to ISO 14229-1 v.2013 (Annex D1) and ISO 15031-5.
Rationale:	ISO 14229-1 v.2013 ISO15031-5
Use Case:	Delete single events: – Support of ´mechanics´ which can follow step by step (DTC by DTC) the repair process Delete event groups: – Support of ´mechanics´ who can delete areas of faults which are subsequent faults of the first one. – OBD faults

Dependencies:	--
Supporting Material:	--

](RS_BRF_02144, RS_BRF_01440)

4.1.4 [SRS_Diag_04067] The DCM and DEM shall provide the diagnostic status information according to ISO 14229-1

[

Type:	Valid
Description:	The DCM and DEM shall provide the diagnostic status information according to the DTCStatusMask, ISO 14229-1 v.2013 (refer to DTC status mask), Annex D5
Rationale:	Advanced fault analysis
Use Case:	Improved fault and event tracking and analysis
Dependencies:	--
Supporting Material:	ISO 14229-1 v.2013

](RS_BRF_02144, RS_BRF_01440)

4.1.5 [SRS_Diag_04139] The DCM and DEM shall support subfunction 0x42 of UDS service 0x19

[

Type:	Valid
Description:	DCM and DEM shall support subfunction 0x42 of UDS service 0x19 to retrieve WWH-OBD-specific DTCs matching the requested DTC status mask and severity mask record.
Rationale:	Support of WWH-OBD
Use Case:	--
Dependencies:	--
Supporting Material:	ISO27145 (WWH-OBD)

](RS_BRF_01440)

4.1.6 [SRS_Diag_04141] The DCM and DEM shall support ISO27145 (WWH-OBD)

[

Type:	Valid
Description:	EURO VI has diagnostic requirements defined in ISO27145 vehicles must comply to.
Rationale:	ISO 14229-1, -2, -5 and ISO 27145-2,-3
Use Case:	Fulfillment of legislative requirements, homologation
Dependencies:	--
Supporting Material:	ISO 14229-1, -2, -5 and ISO 27145-2,-3

](RS_BRF_02184, RS_BRF_01440)

4.1.7 [SRS_Diag_04129] The DCM and DEM shall provide OBD-specific configuration capabilities

[

Type:	Valid
Description:	The DCM and DEM shall provide the following configuration capabilities: • OBD- ECU kind 1: ECU acts as OBD Master ECU (“Master or Primary

	ECU") • OBD- ECU kind 2: ECU acts as OBD Slave ECU ("Dependent / Secondary ECU") • OBD- ECU kind 3: ECU acts as non-OBD ECU The DCM and the DEM shall both provide corresponding configuration parameters to switch on/switch off module-specific OBD functionality. Depending on the configured use case, the associated DCM and DEM port interfaces shall be provided to connect different OBD-ECU kinds on application level (via bus-communication).
Rationale:	UseCase-specific module configuration
Use Case:	Optimization of RAM/ROM consumption
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.1.8 [SRS_Diag_04097] Decentralized modular diagnostic configuration of SW-Cs

[

Type:	Valid
Description:	Each SW-C provides additional diagnostic configuration information for other SW-Cs and for diagnostic modules. The DCM and the DEM module shall be able to generate ports to be connected between these modules in order to allow for diagnostic data to be accessible through the DCM (if requested by an external scan tool) and the DEM (for triggering event entries and collecting event related data).
Rationale:	Because of decentralized configuration & interface requirements each SW-C shall provide and implement diagnostic interfaces to allow code generation and port connection in the DCM (DSP).
Use Case:	Use-case example: • As of today functions and associated diagnostics are developed by several parties. Thus for each function and its diagnostic monitors (e.g. torque management in an engine controller) the diagnostic capabilities are defined separately and will not necessarily be coordinated during development. • System integration and combination of diagnostics for accessibility through DCM and DEM requires that the individual functions and diagnostic features are connected to be compiled as a complete diagnostic system (which is in case of OBD2 certification relevant.) Use-case summary: 1. develop decentralized modular software and its diagnostics without permanent interaction with other SW-Cs developers 2. Combine modules and extract module-specific diagnostic data 3. link diagnostic data from SW-Cs to DCM and DEM
Dependencies:	--
Supporting Material:	ISO 14229-1 v.2013 RS_BRF_00027 RS_BRF_00229

](RS_BRF_02144, RS_BRF_01440, RS_BRF_02200)

4.2 Diagnostic Event Manager (DEM)

4.2.1 [SRS_Diag_04002] The Diagnostic event (fault) management shall be established as Basic SW Module

[

Type:	Valid
Description:	The Diagnostic event (error) management shall be a Basic SW Module described in the Diagnostic WP. Diagnostic event (error) management is out of scope for Mode Management
Rationale:	SW Architecture
Use Case:	Improved fault and event tracking and analysis for Service, assembly line, OBD-SCAN-Tool
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.2 [SRS_Diag_04057] The DEM shall support a classification of events for series production, OBD and expert usage

[

Type:	Valid
Description:	The DEM shall support a classification of events for the following types of events: • Events that are defined for error analysis in the service station shall be stored in the primary event memory. • Events that are defined for detailed error analysis by experts in the after sale department are stored in the secondary error memory. Errors that occur during the development process shall be stored in the DET. Therefore, a special DET API shall be used which is not provided by the DEM.
Rationale:	After sales analysis
Use Case:	Distinction between service station relevant and after sales relevant events.
Dependencies:	--
Supporting Material:	--

](RS_BRF_02168, RS_BRF_02176)

4.2.3 [SRS_Diag_04061] The DEM shall provide mechanisms to distinguish between the reported fault of different applications and basic software modules

[

Type:	Valid
Description:	The DEM shall process event information of different applications (SW-Cs) and BSW modules. Therefore a unique identifier is required to distinguish between different function calls using the same interface. .
Rationale:	Introduce unique event identifiers (EventId) in DEM
Use Case:	Distinction between different applications using the same DEM by their application function group in case of merged applications on one single ECU.
Dependencies:	--
Supporting Material:	--

](RS_BRF_02168)

4.2.4 [SRS_Diag_04063] The DEM module shall process a dedicated event identifier (EventId) for each monitoring path to support an autonomous handling of different events/faults

[

Type:	Valid
Description:	For the internal administration the DEM needs a unique identification of each monitoring path. This identification shall be handled via an Event ID value (Integer).
Rationale:	Introduce unique event indentifiers (EventIds) in DEM
Use Case:	Unique fault identification which can be used for enhanced debugging.
Dependencies:	--
Supporting Material:	--

](RS_BRF_02168)

4.2.5 [SRS_Diag_04066] The DEM module shall provide different event memories which have to be configurable per event

[

Type:	Valid
Description:	The DEM module shall provide different event memories (e.g. primary, mirror, secondary, permanent) supporting the development phase or product improvements as well as the service applications: • The service station has only access to the primary event memory. • The development departments of the OEMs and Suppliers needs access to all configured event memories. The different event memories allow the storage of development events and they are not suited as a trace tool.
Rationale:	Advanced fault analysis
Use Case:	The development departments of the OEMs and Suppliers need as much as possible deeper fault/event analysis although the mechanics may have deleted the faults or may not need to know if there are more detailed root causes for an event or fault
Dependencies:	--
Supporting Material:	--

](RS_BRF_02200)

4.2.6 [SRS_Diag_04133] The DEM module shall support Aging

[

Type:	Valid
Description:	The DEM module shall support Aging to remove event memory entries from the event memory which have not failed for a specific number of operating cycles.
Rationale:	Remove information from fault memory that is not relevant for a repair action.
Use Case:	Network timeout fault that has been detected, but is not in active state any more.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.7 [SRS_Diag_04140] Support of aging for UDS status bits “confirmedDTC” and “testFailedSinceLastClear”

[

Type:	Valid
Description:	The DEM module shall provide the capability to age both the confirmedDTC bit and the testFailedSinceLastClear bit after a configurable number of aging cycles has been reached. The value at which each bit is aged may be different between the two.
Rationale:	--
Use Case:	--
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.8 [SRS_Diag_04136] Support of configurable “confirmed” threshold

[

Type:	Valid
Description:	The DEM shall support a postbuild configurable “confirmed” threshold.
Rationale:	Flexible usage of local legislated requirements.
Use Case:	In different markets (US/EURO), the DEM needs to support different legislated requirements. For the US market the MIL and the ConfirmedDTC is activated after 2 DCY (Driving Cycles). For the EUR market the MIL and the ConfirmedDTC is activated after 3 DCY (Driving Cycles).
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.9 [SRS_Diag_04068] The DEM module shall provide event specific debounce algorithms

[

Type:	Valid
Description:	The DEM module shall support event specific debounce counters to improve signal quality internally. The configuration of the DEM module shall support the following types of debounce mechanisms: • counter based • time based • handling of external debouncing The DEM module shall provide the ability to configure the jump behavior including jump up and jump down threshold value of the debounce counter in case of pre-passed or pre-failed event reporting. If failure detection jitters (e.g. sporadically reported pre-passed events), failure detection must not be delayed or prevented. For example, a monitoring configuration does NOT use jumpdown to avoid losing an event reporting a pre-failed status. The provision of jumping behavior of the debounce counter shall ensure the failure detection time because debouncing always starts from a defined starting point.

Rationale:	Advanced fault analysis
Use Case:	All SW-Cs and BSW modules can report events to the DEM module. The diagnostic module processes all these events and is able to provide a central de-bounce behavior for event classification & status management.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02144)

4.2.10 [SRS_Diag_04125] The behaviour of the event debounce counter shall be configurable

[

Type:	Valid
Description:	It shall be configurable if the debounce counter shall be frozen or reset, when at least one enable condition for the event is set to "not fulfilled" or when ControlDTCSetting is set to “disabled”. In case of switching the enable conditions to “fulfilled” the monitor needs to be informed to restart the event detection. In case of switching ControlDTCSetting to “re-enabled” the monitor needs to be informed to restart the event detection.
Rationale:	Flexible usage of DEM internal debouncing
Use Case:	--
Dependencies:	--
Supporting Material:	--

](RS_BRF_02144)

4.2.11 [SRS_Diag_04124] The DEM shall be able to store the current debounce counter value non-volatile to over a power-down cycle

[

Type:	Valid
Description:	The DEM shall be able to store the current debounce counter value non-volatile to over a power-down cycle.
Rationale:	Support of DTC de-bouncing within several power cycles.
Use Case:	While the typical DTC operation cycle for a DTC is to start at power up and end at power down, there are different situations, when a particular DTC must define its operation cycle to span multiple ECU power up/down cycles. In this case, the FDC would need to be stored in NVM as it may never make it to 127 during a single power up.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02144)

4.2.12 [SRS_Diag_04118] The DEM shall optionally support event displacement

[

Type:	Valid
Description:	The DEM shall optionally support event displacement. The following sequence of different displacement criteria shall be possible: 1. Priority 2. Active/passive status (optional)

	3. Occurrence
Rationale:	Limited hardware (memory ressources) in ECU
Use Case:	Error memory is full and valid event is reported to DEM
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.13 [SRS_Diag_04069] The DEM module shall provide event specific information of warning indicators requested by SW-Cs or other BSW modules

[

Type:	Valid
Description:	The DEM module is able to activate or deactivate indicators (e.g. lamps, text message, beep) per event stored in the configured event memory. The information on indicators is requested by SW-Cs or other BSW modules to process further calculation or react on the received result.
Rationale:	Information distribution to the SW-Cs and BSW modules
Use Case:	Indications of the Malfunction Indicator Lamp (MIL)
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02144)

4.2.14 [SRS_Diag_04070] The DEM module shall process the order of the event occurrences in an appropriate and obvious manner

[

Type:	Valid
Description:	- The occurrence order shall be recognizable by e.g. time stamps or age. (storage of events shall be connected to age or timestamp) - Reoccurrence of events takes over the old position of the event - Reoccurrence of healed events are handled as valid events.
Rationale:	Advanced fault analysis
Use Case:	Improved clustering and judging of events
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

](RS_BRF_01440, RS_BRF_01326)

4.2.15 [SRS_Diag_04071] The DEM module shall process events according to their defined importance like priority and/or severity

[

Type:	Valid
Description:	The events shall be sorted or assigned to a specific priority (e.g. Severity Mask – ISO14229-1 v.2013,Annex D3) representing their importance like: - Healed events can be overwritten - Privileged storing in case of Event Buffer filled up with less privileged events
Rationale:	ISO14229-1 v.2013
Use Case:	Improved clustering and judging of events
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

](RS_BRF_01440)

4.2.16 [SRS_Diag_04072] The DEM shall provide additional event information to report the occurrence of an event by km-stamp, driving cycles or time

[

Type:	Valid
Description:	Fault duration e.g. by km-stamp, driving cycles or time - Between failed and passed - Since failed - Since last clear
Rationale:	Advanced fault analysis
Use Case:	Improved clustering and judging of events/faults
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

](RS_BRF_01440)

4.2.17 [SRS_Diag_04073] DEM shall process combined events which shall consist of several different events

[

Type:	Valid
Description:	The DEM shall allow for combining several individual events to a different representing (combined) event that has its own event ID. The configuration of the DEM shall allow for enabling and disabling the support for “combined diagnostic events”. If “combined diagnostic events” are supported the configuration of the DEM shall allow for assigning each “diagnostic event” the attribute “combined diagnostic event ID”.
Rationale:	Advanced fault analysis
Use Case:	Improved clustering and judging of events/faults. Several internal hardware faults of an electronic control unit can be mapped onto a single “ECU internal” failure to reduce the number of Diagnostic Trouble Codes shown to the technician in the service workshop.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.18 [SRS_Diag_04074] The DEM module shall process event related data (e.g. freeze frames and extended data records)

[

Type:	Valid
Description:	The DEM module shall be able to store different sets of environmental data (freeze frames or extended data records) per event. The point in time when the event related data is captured, updated or stored (e.g. depending on status bit transition of the UDS DTC status byte) shall be configurable (limited to common use-cases or definitions of ISO 14229-1 v.2013). Based on the configuration the DEM module shall be able to access data elements provided by SW-Cs or other BSW modules of freeze frames or extended data records.
Rationale:	Advanced fault analysis

Use Case:	Improved clustering and judging of events/faults
Dependencies:	SRS_Diag_04024
Supporting Material:	--

](RS_BRF_01440)

4.2.19 [SRS_Diag_04134] The DEM shall be able to store internal data to Extended Data Records and Snaphot Records

[

Type:	Valid
Description:	The DEM shall provide the capability to store internal data to Extended Data Records and Snapshot Records. This means that DEM-internal data elements like Operation Cycle Counter, Fault Detection Counter (FDC) and Occurrence Counter can be assigned to environmental data records.
Rationale:	Some data objects that are internally generated by the DEM can be retrieved by service $19.
Use Case:	Reading Operation Cycle Counter, Fault Detection Counter and Occurrence Counter
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

](RS_BRF_01440)

4.2.20 [SRS_Diag_04127] Configurable record numbers and trigger options for DTCSnapshotRecords and DTCExtendedDataRecords

[

Type:	Valid
Description:	The DEM module shall provide the capability to configure record numbers and trigger options for the storage of DTCSnapshotRecords and DTCExtendedDataRecords.
Rationale:	Advanced fault analysis
Use Case:	Flexible handling of DTCSnapshotRecords and DTCExtendedDataRecords
Dependencies:	SRS_Diag_04074
Supporting Material:	--

](RS_BRF_01440)

4.2.21 [SRS_Diag_04079] The size of a FreezeFrame shall be reported to the DCM by the DEM

[

Type:	Valid
Description:	If the DEM module is requested to support freeze frames, the DEM module shall be able to determine the size of a FreezeFrame and to provide this information via API call.
Rationale:	The DCM requires this information due to the allocation of memory space for the storage of the FreezeFrame information.
Use Case:	An external testing tool connected to the vehicle requests currently stored error codes and the corresponding environmental data.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.22 [SRS_Diag_04104] The DEM module shall support a signal based configuration of event related data (define freeze frames and extended data records)

[

Type:	Valid
Description:	--
Rationale:	Advanced fault analysis
Use Case:	A SW-C or other a BSW modul provides diagnostic signals (data elements) which will be merged to different data identifiers (DIDs).
Dependencies:	--
Supporting Material:	Refer to concept “Functional diagnostics of SW-Cs”, ServiceNeeds described in SW-C Template, RS_BRF_00230

](RS_BRF_01440)

4.2.23 [SRS_Diag_04075] The DEM module shall support a configuration to assign specific event to a customer specific DTC

[

Type:	Valid
Description:	Assignment of events (reported by SW-Cs or BSW modules) to customer specific / standardized DTC’s which shall be configurable related to number of DTCs.
Rationale:	The event identifier is used DEM internally only. An external scan tool requests a DTC number which was assigned to one specific or several events (combined events).
Use Case:	The DTC number is used for external fault analysis and is reported by the DCM module if a connected scan tool requests fault memory information (e.g. service $19 to read DTC information).
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.24 [SRS_Diag_04076] The DEM module shall provide a set of system cycles that may qualify the event in an additional manner

[

Type:	Valid
Description:	The cycles are used for event qualification, event aging or warning indicator handling.Typical cycles are: - driving cycle - engine warm up cycle - ignition on off cycle - power up power down cycle - operation active passive cycle - in or out of voltage range cycle
Rationale:	Event status management, ISO14229-1 v.2013
Use Case:	Improved clustering and judging of events/faults
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.25 [SRS_Diag_04123] The DEM module shall support harmonized Driving-/WarmUp cycles

⌈

Type:	Valid
Description:	The DEM module shall support harmonized Driving-/WarmUp cycles. The calculation of Driving-/WarmUp cycles is based on legal requirements.
Rationale:	OBD certification requires vehicle consistent calculations based on a harmonized Driving-/WarmUp cycle in the centralized OBD Master ECU.
Use Case:	Qualification of OBD-relevant DTCs
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440)

4.2.26 [SRS_Diag_04091] Notifications about valid freeze frame data

⌈

Type:	Valid
Description:	The DEM shall be enabled to notify other SW-C (or BSW modules) about valid freeze frame data (e.g. time stamp). If this functionality is configured for an event, it shall be executed on each entry of a valid freeze frame of this event into the event memory.
Rationale:	In the current version of the DEM SWS, there is no possibility to provide freeze frame data (like time stamp) to another SW-C / BSW module beside the DCM. Additionally this functionality provides a simple way for supporting this data to other components (at every time, where valid data are available), so that no cyclic polling is needed.
Use Case:	The information provided by this functionality is needed by modules like a special ‘Diagnostic active response handler’.
Dependencies:	--
Supporting Material:	RS_BRF_00231

⌋(RS_BRF_01440)

4.2.27 [SRS_Diag_04092] Control of event handling

⌈

Type:	Valid
Description:	The DEM shall provide locking functionality for dedicated events. If this functionality is configured for an event, it shall be called before clearing this event from the event memory. Unless the functionality does not allow clearance, the event must not be cleared.
Rationale:	If the environmental conditions do not allow the clearance of an event, the application must have the opportunity to prohibit the deletion.
Use Case:	Some dedicated events must never get cleared from event memory, while the ECU is in a special operation mode (e.g. assembly-, transport-, or flash-mode).
Dependencies:	--
Supporting Material:	

⌋(RS_BRF_01440, RS_BRF_02168)

4.2.28 [SRS_Diag_04093] Memory Overflow indication

⌈

Type:	Valid
Description:	For each Event Memory it shall be indicated if the related event memory (e.g. primary, secondary, mirror) is full and the next event occurs to be stored in this event memory.
Rationale:	The information that an event memory overflow occurred is very important for fault analysis.
Use Case:	• Triggering further internal behavior of the DEM module (e.g displacement strategies) • Linking this information to a dedicated Extended Data Record • Vendor specific UDS-Service
Dependencies:	--
Supporting Material:	

⌋(RS_BRF_01440)

4.2.29 [SRS_Diag_04095] The DEM module shall provide the ability to handle event specific enable and storage conditions

⌈

Type:	Valid
Description:	Depending on environmental data or the current status of an ECU the DEM module considers a certain number of conditions/checks before the event get qualified. • Enable condtions affects the ability of a diagnostic monitor to report events • Storage conditions affects the qualification of the reported event before the event is stored in its configured event memory
Rationale:	Support mechanisms to avoid reams of event memory entries in case of specific ECU conditions.
Use Case:	For specific fault groups (e.g. network faults) it is necessary to evalute the current status of an ECU (e.g. undervoltage) before the reported events are qualified by the DEM module.
Dependencies:	--
Supporting Material:	

⌋(RS_BRF_02144)

4.2.30 [SRS_Diag_04096] The DEM module shall support the UDS DTC status bit support & handling according to ISO14229-1

⌈

Type:	Valid
Description:	The DEM module shall provide the ability to handle the UDS DTC status bit information according to ISO14229-1 v.2013.
Rationale:	UDS DTC status bit transitions are defined in ISO14229-1 v.2013.
Use Case:	Provide the UDS DTC status bit information requested by a scan tool.
Dependencies:	--
Supporting Material:	ISO 14229-1 v.2013

⌋(RS_BRF_02144)

4.2.31 [SRS_Diag_04109] The DEM module shall provide an interface to retrieve the number of event memory entries

⌈

Type:	Valid
Description:	The DEM module shall provide an interface to retrieve the number of event memory entries currently stored in Primary, Secondary and Mirror Memory to the application. Additionally, the corresponding Client Server Interface shall be provided.
Rationale:	The interface is required from application, to check if event memory entries exist that influence the ECU behavior.
Use Case:	There is an application message where a status bit must be set as soon as events are stored in the event memory. Therefore, the application needs to know how many event memory entries exist in the DEM.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_02144)

4.2.32 [SRS_Diag_04105] Event memory management

⌈

Type:	Valid
Description:	The DEM module shall be able to handle valid events, update existing event memory entries or replace events in case of a full event memory. The processing is triggert externally (e.g. by the reported event status) or depends on internal information (e.g. value of debounce counter/timer, occurrence counter, …)
Rationale:	Support of fault storage and analysis
Use Case:	Support of fault storage and analysis
Dependencies:	--
Supporting Material:	ISO 14229-1 v.2013

⌋(RS_BRF_02144)

4.2.33 [SRS_Diag_04102] The DEM module shall provide a chronological reporting order of the events located in the configured event memory

⌈

Type:	Valid
Description:	The DEM module is able to handle the occurrence of events (e.g. represented by a time stamp or odometer value) refer to 4.2.14. If the DCM module requests fault information, the DEM module shall reports all faults, which fits to the configured status mask, in a defined chronological order.
Rationale:	Advanced fault analysis
Use Case:	Advanced fault analysis
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440)

4.2.34 [SRS_Diag_04099] The DEM should forward incoming events to the DLT interface

[

Type:	Valid
Description:	The DEM should forward error events to the DLT.
Rationale:	To have an overview of all log, trace error messages and to set all of them in the correct context with the error events reported to the DEM, it is important to have all this messages and events in one list (context). This makes an analysis of the reported errors more efficient and gives a correct picture of the ongoing sequences, which report an error.
Use Case:	• a SWC or BSW module sets an DTC in the DEM • the DEM forwards this event to the DLT • the DLT turns these events in the DLT format and sends it over the a network interface to a DLT client (PC)
Dependencies:	--
Supporting Material:	--

](RS_BRF_02240)

4.2.35 [SRS_Diag_04107] Defensive behavior of the DEM module

[

Type:	Valid
Description:	For safety-related applications, the Diagnostics Event Manager shall ensure data integrity of errors information stored in non-volatile memory.
Rationale:	Protection of error events memory is needed for safety-related
Use Case:	Error events memory could have been corrupted
Dependencies:	--
Supporting Material:	Use the optional CRC and redundancy capabilities provided by the NVRAM Manager for Diagnostics Event Manager NVRAM Blocks. Only blocks assigned to error events of high severity can be protected. These blocks can be stored in non-volatile memory when the error event is confirmed (before shutdown of the ECU), refer to RS_BRF_00129

](RS_BRF_01840)

4.2.36 [SRS_Diag_04126] Configurable suppression of events

[

Type:	Valid
Description:	The DEM shall provide a postbuild/loadable boolean configuration option per event. If the DemEventParameterSuppressed is set to true the event behaves the same as if it is suppressed by API call. An event suppressed by configuration can not be activated via API call.
Rationale:	Use case-specific configuration of fault memory, only required events are visible and usable in ECU.
Use Case:	Variant coding
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.37 [SRS_Diag_04110] The DEM module shall support SAE J1939 lamp status

[

Type:	Valid
Description:	The composite and DTC-specific lamp status of the following lamps shall be supported: Malfunction Indicator Lamp, Red Stop Lamp, Amber Warning Lamp and Protect Lamp.
Rationale:	Support of SAE J1939-73
Use Case:	Diagnostics in HDV, HD-OBD
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02144)

4.2.38 [SRS_Diag_04111] The DEM module shall support SAE J1939 Expanded- / FreezeFrame

[

Type:	Valid
Description:	Individual configuration of FreezeFrame and Expanded FreezeFrame; Expanded FreezeFrame shall be SPN-based.
Rationale:	Support of SAE J1939-73
Use Case:	Diagnostics in HDV, HD-OBD
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02144)

4.2.39 [SRS_Diag_04117] The DEM shall provide a configurable behavior for the deletion of DTC

[

Type:	Valid
Description:	Usually, only ClearAllDTCs is used for the deletion of DTCs. Therefore, the DEM shall provide a configurable behavior which optionally limits the deletion of DTCs to ClearAllDTCs.
Rationale:	OEM specific behavior
Use Case:	Allow only ClearAllDTCs and therefore optimization of ClearDTC behavior
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.40 [SRS_Diag_04122] The ClearDTC command in DEM shall be usable for a Complex Device Driver

[

Type:	Valid
Description:	To be able to clear DTCs in Secondary and Mirror Memory the ClearDTC command in DEM shall be usable for a Complex Device Driver. The access to clear DTCs via DCM (UDS service $14) is limited to Primary Memory.
Rationale:	Provision of ClearDTC in DEM to other calling instances beside DCM
Use Case:	Deletion of Primary Memory by different calling instance than DCM and deletion of Secondary and Mirror Memory
Dependencies:	--

Supporting Material:	--

](RS_BRF_01440)

4.2.41 [SRS_Diag_04112] The DEM module shall support DTCs according to SAE J1939

[

Type:	Valid
Description:	The DEM module shall support DTCs according to SAE J1939-73.
Rationale:	Support of SAE J1939-73
Use Case:	Diagnostics in HDV, HD-OBD
Dependencies:	DEM, J1939DCM
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02144)

4.2.42 [SRS_Diag_04113] The DEM module shall support a set of SAE J1939 DM-messages

[

Type:	Valid
Description:	The following DM-messages shall be supported: **Name Description** DM01 Active Diagnostic Trouble Codes DM02 Previously Active Diagnostic Trouble Codes DM03 Diagnostic Data Clear/Reset for Previously Active DTCs DM04 Freeze Frame Parameters DM05 Diagnostic Readiness 1 DM06 Emission Related Pending DTCs DM11 Diagnostic Data Clear/Reset for Active DTCs DM12 Emissions Related Active DTCs DM13 Stop Start Broadcast DM19 Calibration Information DM20 Monitor Performance Ratio SAE J1939-73 Revised SEP2006 DM21 Diagnostic Readiness 2 DM23 Previously Active Emission Related Faults DM24 SPN Support DM25 Expanded Freeze Frame DM26 Diagnostic Readiness 3 DM28 Permanent DTCs DM29 Regulated DTC Counts (Pending, Permanent, MIL-On, PMIL-On) DM31 DTC to Lamp Association DM35 Immediate Fault Status
Rationale:	Support of SAE J1939-73
Use Case:	Diagnostics in HDV, HD-OBD
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02144)

4.2.43 [SRS_Diag_04130] The DEM shall provide the capability to process a new request

⌈

Type:	Valid
Description:	If the DEM is executing an asynchronous request and meanwhile gets a new request with a different parameter set, the Dem shall immediately process the new request without issuing a negative response.
Rationale:	During diagnostic sessions, a running protocol may be cancelled and another protocol with higher priority is started.
Use Case:	Abortion of request with low priority to process a request with higher priority.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440)

4.2.44 [SRS_Diag_04131] Event management mechanisms in DEM

⌈

Type:	Valid
Description:	All memory locations except mirror memory provided by the DEM shall use the same event management mechanisms.
Rationale:	Ensure identical event management behavior.
Use Case:	--
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440)

4.2.45 [SRS_Diag_04137] Definition of replacement failure in DEM

⌈

Type:	Valid
Description:	Upon filtering the storage of failure reports by central conditions (Storage Condition), it shall be possible to define and store a replacement failure info which then can be stored to the event memory. This replacement failure will represent the actual failure reason.
Rationale:	Improvement of failure analysis.
Use Case:	--
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440)

4.2.46 [SRS_Diag_04142] The DEM module shall support component dependencies

⌈

Type:	Valid
Description:	The actually monitored components like hardware parts (sensors, actuators) or monitored signals along with their inter-dependencies shall be representable in the diagnostic system. For each component the status information shall be provided for system degradation and the failure storage shall consider the dependencies for deciding upon storing failures.
Rationale:	Avoid irrelevant failure storage. Furthermore facilitate correct status calculation of components and system reconfiguration.

Use Case:	For large systems it becomes difficult to consider all the dependencies and relations which are relevant for system reconfiguration and determination of failure root causes. This is improved by a hierarchical representation of component and their dependencies.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.2.47 Interfaces and APIs

4.2.47.1 [SRS_Diag_04077] The DEM uses standard mechanisms provided by NVRAM-Manager

[

Type:	Valid
Description:	--
Rationale:	Non volatile data storage
Use Case:	The DEM triggers data storage during normal ECU operation to avoid loss of volatile data / event information.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01928)

4.2.47.2 [SRS_Diag_04030] The DEM shall provide an interface via the RTE to monitoring SW components for reporting and processing diagnostic test results

[

Type:	Valid
Description:	The DEM shall provide via the RTE an Interface to Monitoring SW Components for reporting and processing diagnostic results. Monitoring SW-components report diagnostic results as soon as valid results are available.
Rationale:	Interface to event generating monitoring SW-Components
Use Case:	Ensure the basic diagnostic functionality
Dependencies:	--
Supporting Material:	--

](RS_BRF_01280)

4.2.47.3 [SRS_Diag_04031] The DEM shall notify the Function Inhibition Manager (FIM) upon changes of the event status in order to process them according to the SW components dependencies

[

Type:	Valid
Description:	Control (enable/disable) of functionalities of SW components based on the following inhibit condition: - faults
Rationale:	DEM information for Inhibition of functions.
Use Case:	Usage of DEM information for Inhibition of functions.
Dependencies:	--
Supporting Material:	--

](RS_BRF_02216)

4.2.47.4 [SRS_Diag_04128] DEM interface to set/reset the WarningIndicatorRequested bit

[

Type:	Valid
Description:	The DEM shall provide an interface to set and reset the WarningIndicatorRequested bit.
Rationale:	Consitency between fail-safe reaction status and fault memory entry.
Use Case:	Setting the WarningIndicatorRequested bit by the fail-safe application according to the current state of the fail-safe reaction to ensure consistency between fail-safe reation and fault memory entry.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.3 Diagnostic Communication Manager (DCM)

4.3.1 [SRS_Diag_04007] The DCM shall provide a diagnostic service handling for the SW-Components which are using the DCM

[

Type:	Valid
Description:	The DCM shall provide the diagnostic service handling, according to ISO14229-1 v.2013, ISO 15031-5 and ISO 15765-3 for the communication between an AUTOSAR conform ECU and an internal tester or an external diagnostic tool.
Rationale:	Only one diagnostic service instance in an ECU.
Use Case:	Communication with an external diagnostic tools in - development - manufacturing - service (garage) - OBD scan tools Communication with an internal tester.
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013 ISO 15031-5 ISO 15765-3

](RS_BRF_01440)

4.3.2 [SRS_Diag_04021] The DCM shall support the handling of different diagnostic sessions in parallel

[

Type:	Valid
Description:	DCM needs to handle an established diagnostic communication and a parallel diagnostic access request in parallel. This is necessary to open a diagnostic access with high priority and the controlled shutdown of the established diagnostic access with low priority.
Rationale:	To prioritize handling of different Diagnostic Protocols e.g. OBD and normal diagnostic communication as UDS.
Use Case:	A internal vehicle diagnostic tester communication is interrupted by OBD diagnostic access request.
Dependencies:	[SRS_Diag_04032] Support of different diagnostic addresses [SRS_Diag_04061] Multiple or parallel usage from different applications of the DEM functionality
Supporting Material:	--

](RS_BRF_01440)

4.3.3 [SRS_Diag_04032] Different diagnostic addresses shall be supported by multiple (physical) channels

[

Type:	Valid
Description:	Modern ECUs contain more than one functionality (e.g. board computer, instrument cluster). Each functionality shall be addressable by a diagnostic tool with a different diagnostic address. This does not imply that those multiple requests are allowed in parallel.
Rationale:	High flexibility and granularity for addressing of SW-Components

Use Case:	At the service (garage) a fault symptom is based on functionality. The service only wants to address this functionality.
Dependencies:	[SRS_Diag_04021] Switch diagnostic communication access
Supporting Material:	--

](RS_BRF_01440)

4.3.4 [SRS_Diag_04058] The DCM module shall be able to access different event memories provided by the DEM module

[

Type:	Valid
Description:	The DCM module shall support diagnostic services to read or remove event entries from the configured event memory seperatly.
Rationale:	Advanced fault analysis
Use Case:	The development departments of the OEMs and Suppliers need as much as possible deeper fault/event analysis although the mechanics may have deleted the faults or may not need to know if there are more detailed root causes for an event or fault.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.3.5 [SRS_Diag_04024] The DCM module shall be able to access and handle specific data elements and data element groups if requested by an external scan tool

[

Type:	Valid
Description:	The DCM module shall provide interfaces for the DEM module and for SW-Cs to access diagnostic data and to proccess diagnostic services. The size of a diagnostic data element is derived from the RTE or provided as an attribute of the API call itself.
Rationale:	Optimized usage of resources.
Use Case:	Transfer environmental / FreezeFrame data between DEM and DCM
Dependencies:	SRS_Diag_04074
Supporting Material:	--

](RS_BRF_01440)

4.3.6 [SRS_Diag_04098] Standard bootloader interaction

[

Type:	Valid
Description:	Integration of a standard bootloader into the AUTOSAR architecture. • If the DCM is requested to change into the programming session ($10 02), the DCM shall either send the final response and then activate the bootloader or it shall not send the final response and activate the bootloader where the activate the bootloader and the final response shall be sent by the bootloader (according HIS [FL-504]). • The DCM shall check the environmental conditions like engine speed before activating the bootloader (Interface already supported in AUTOSAR 3.0). • The behavior of the DCM to optionally issue a NRC 0x78 (RCRRP, retrigger the timeout supervision of the diagnostic client) during transition to the bootloader shall be configurable.

Rationale:	Bootloader concept has to be standardized within AUTOSAR.
Use Case:	Usage of “off-the-shelf” boot loader
Dependencies:	--
Supporting Material:	--

](RS_BRF_02152)

4.3.7 [SRS_Diag_04100] The DCM shall provide an interface for DLT to transport log and trace data over a diagnostic service

[

Type:	Valid
Description:	DCM should provide an interface for DLT to send and receive data over the diagnostic service. Logging and tracing data are sent over this service and control requests for DLT are received. For this purpose the DCM should implement the ResponseOnEvent service (see UDS spec.). DCM should provide an interface for DLT to send data and receive control requests.
Rationale:	Log&Trace needs an interface to send Log&Trace data out of the ECU. DCM provides a bus independent access to the ECU over standardized diagnostic. This is available during production phase and provides a secured session control. Because log and trace messages are event triggered and the storage on the ECU is limited, these messages must be sent when they occur.
Use Case:	• Transmitting log and trace data during a diagnostic session • Advanced Diagnostic Tracing, optional over telematic services
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.3.8 [SRS_Diag_04015] The DCM shall support timing handling according to ISO15765-3

[

Type:	Valid
Description:	In ISO15765-3 timing handling for physical and functional communication is described. Also how to react on errors. DCM shall work according this specification. Timing parameters shall be configurable (see dependencies).
Rationale:	Ensure a steady and save communication link and guarantee specified timing conditions.
Use Case:	Optimizing of timing for high performance during reprogramming.
Dependencies:	[SRS_Diag_04059] Configuration of timing parameter
Supporting Material:	ISO15765-3

](RS_BRF_01440)

4.3.9 [SRS_Diag_04000] The DEM and DCM shall support the Diagnostic Standard UDS (ISO14229-1)

[

Type:	Valid
Description:	The DEM and DCM shall support all diagnostic services of UDS Standard (ISO14229-1 v.2013).
Rationale:	Use standardized diagnostic services for communication between the ECU and an external scan tool.

Use Case:	Diagnostics with a UDS tester/scan tool
Dependencies:	--
Supporting Material:	ISO 14229-1 v.2013

](RS_BRF_01440, RS_BRF_02144)

4.3.10 [SRS_Diag_04135] The DCM shall support UDS service $38 (RequestFileTransfer)

[

Type:	Valid
Description:	The DCM shall support UDS service 0x38 (“RequestFileTransfer”).
Rationale:	The requestFileTransfer service is used by the client to initiate a file data transfer from either the client to the server or from the server to the client (download or upload). Additionally, this service has capabilities to retrieve information about the file system.
Use Case:	Upload of files (e.g. data files, graphics, …)
Dependencies:	--
Supporting Material:	ISO 14229-1

](RS_BRF_01440)

4.3.11 [SRS_Diag_04001] The DEM and DCM shall support the Diagnostic Standard OBD (ISO15031-5)

[

Type:	Valid
Description:	The DEM and DCM shall support all services of OBD Standard (ISO15031-5).
Rationale:	This standard is required for emission related control units by law
Use Case:	Diagnostic with a OBD Tester (e.g. Scan Tool)
Dependencies:	--
Supporting Material:	ISO15031-5

](RS_BRF_01440, RS_BRF_02144)

4.3.12 [SRS_Diag_04005] The DCM shall manage Security Access level handling

[

Type:	Valid
Description:	The DCM shall manage the handling of the UDS-service SecurityAccess (0x27) and also the Security level handling. The accessibility of the services (service identifier) in the actual security level shall be checked by the DCM
Rationale:	Some diagnostic services are in dependence to a security access level. Therefore it is necessary that the DCM has knowledge about the current level and no service which is restricted by security will be processed without authorization.
Use Case:	Not all diagnostic services are allowed in each security level.
Dependencies:	[SRS_Diag_04000] Support Diagnostic Standard UDS
Supporting Material:	--

](RS_BRF_01440)

4.3.13 [SRS_Diag_04006] Session handling is managed by DCM

⌈

Type:	Valid
Description:	The DCM shall support the transition from a default session to any other session, also back to the default session. (A diagnostic session enables a specific set of diagnostic services and/or functionality).
Rationale:	Some diagnostic services are not available in the default session. Therefore it is necessary that the DCM has knowledge about the current session and no service which is connected to a non default session will be processed in the default session.
Use Case:	Special services need a different session than the default session, e.g. Reduction of communication traffic on the network in order to get more performance for the flash programming.
Dependencies:	[SRS_Diag_04000] Support Diagnostic Standard UDS [SRS_Diag_04005] SecurityAccess level handling is managed by DCM
Supporting Material:	--

⌋(RS_BRF_01440)

4.3.14 [SRS_Diag_04016] The DCM shall support “Busy handling” by sending a negative response 0x78

⌈

Type:	Valid
Description:	DCM shall provide the sending of the negative response 0x78 in order get more time to build up the final positive or negative response.
Rationale:	Ensure a steady and save communication link and guarantee specified timing conditions.
Use Case:	When an application cannot provide the response in the protocol specific time.
Dependencies:	[SRS_Diag_04000] Support Diagnostic Standard UDS
Supporting Material:	ISO15765-3 ISO14229-1 v.2013

⌋(RS_BRF_01440)

4.3.15 [SRS_Diag_04119] The DCM shall handle the execution of diagnostic services according to the assigned diagnostic session

⌈

Type:	Valid
Description:	If the current diagnostic session transitions to a different session (initiated by UDS Service $10 DiagnosticSessionControl), the DCM shall only maintain active diagnostic functionality if supported in the valid session and if not prohibited by security access.
Rationale:	No interruption of diagnostic functionality
Use Case:	Deactivation of fault management and normal communication during ECU reprogramming
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

⌋(RS_BRF_01440)

4.3.16 [SRS_Diag_04019] The DCM shall confirm transmitting if complete to continue processing

⌈

Type:	Valid
Description:	In some cases it is necessary that the application starts execution of the requested functionality after the positive response is completely transmitted. The application needs the callback functionality to get the information that the positive response is complete transmitted. After this callback the application can execute the requested functionality.
Rationale:	This behavior is specified by ISO 14229-1 v.2013.
Use Case:	E.g. call of the reset function. This call needs to be done after transmission of the positive response is over.
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

⌋(RS_BRF_01440)

4.3.17 [SRS_Diag_04020] DCM shall suppress responses to diagnostic tool requests

⌈

Type:	Valid
Description:	DCM shall suppress responses in following cases: - Suppress positive response (SuppressPosRequest Bit set) - Suppress negative responses (NRC 11, 12 and 31 at functional addressing)
Rationale:	This behavior is specified by ISO 14229-1. Prevent bus burst as result of a functional request.
Use Case:	--
Dependencies:	[SRS_Diag_04000] Support Diagnostic Standard UDS
Supporting Material:	ISO14229-1 v.2013 ISO15031-5

⌋(RS_BRF_01440)

4.3.18 [SRS_Diag_04033] The DCM shall support the upload/download services for reading/writing data in an ECU in an extended and manufacturer specific diagnostic session

⌈

Type:	Valid
Description:	The UDS services RequestDownload, RequestUpload, TransferData, RequestTransferExit (0x34-0x37) are used for data handling, e.g. accessing NVRAM. This does not interfere the reprogramming, because this is handled by the bootloader.
Rationale:	Enable a possibility to modify set of parameters.
Use Case:	End of line configuration in the manufacturing.
Dependencies:	[SRS_Diag_04000] Support Diagnostic Standard UDS
Supporting Material:	ISO14229-1 v.2013

⌋(RS_BRF_01440)

4.3.19 [SRS_Diag_04036] The DCM shall check the format of diagnostic service

[

Type:	Valid
Description:	The format checking shall include the service identifier (SID). Existing sub-service identifier shall be checked. The checks shall include the following attributes: - diagnostic session level - diagnostic security level - message length Note: Further checking is done by the application.
Rationale:	The application won't get a request with incorrect format.
Use Case:	Failure Handling in communication.
Dependencies:	[SRS_Diag_04000] Support Diagnostic Standard UDS
Supporting Material:	ISO14229-1 v.2013

](RS_BRF_01440, RS_BRF_02232)

4.3.20 [SRS_Diag_04115] The optional parameter DTCSettingControlOptionRecord as part of UDS service ControlDTCSetting shall be limited to GroupOfDTC

[

Type:	Valid
Description:	ISO14229-1 does not specify how the parameter DTCSettingControlOptionRecord needs to be used. Therefore, the usage of the parameter shall be limited to GroupOfDTC.
Rationale:	Currently, no other use case for parameter DTCSettingControlOptionRecord is known than the usage for GroupOfDTC.
Use Case:	Fault storage is activated and deactivated for one specific DTC or for all DTCs.
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

](RS_BRF_02160)

4.3.21 [SRS_Diag_04120] The DCM shall support a predefined AddressAndLengthFormatIdentifier

[

Type:	Valid
Description:	The DCM shall support a predefined AddressAndLengthFormatIdentifier for UDS service $23 (ReadMemoryByAddress), UDS service 0x2C (DynamicallyDefineDataIdentifier with subservice DefineByMemoryAddress), UDS service 0x3D (WriteMemoryByAddress), UDS service 0x34 (RequestDownload) and UDS service 0x35 (RequestUpload).
Rationale:	AddressAndLengthFormatIdentifier is defined once in DCM and afterwards used in corresponding UDS services.
Use Case:	Static configuration of AddressAndLengthFormatIdentifier
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

](RS_BRF_01440, RS_BRF_01024)

4.3.22 [SRS_Diag_04121] The DCM shall provide the handling of service DynamicallyDefineDataIdentifier according to ISO 14229-1

⌈

Type:	Valid
Description:	The DCM shall provide the handling of service DynamicallyDefineDataIdentifier according to ISO 14229-1 v.2013.
Rationale:	Standardized ISO 14229-1 v.2013 behavior
Use Case:	--
Dependencies:	--
Supporting Material:	ISO14229-1 v.2013

⌋(RS_BRF_01440, RS_BRF_02144)

4.3.23 [SRS_Diag_04138] Limitatation of execution of diagnostic requests

⌈

Type:	Valid
Description:	The DCM shall provide the capability to limit the execution of diagnostic services by using “Prerequisite Conditions”. On each service request the DCM may check "mode dependencies" or "environmental conditions".
Rationale:	--
Use Case:	Limit the request execution due to vehicle- or ECU states/-conditions.
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440)

4.3.24 Interfaces and APIs

4.3.24.1 [SRS_Diag_04078] The DCM shall use a common API of the diagnostic event manager to access the fault memory

⌈

Type:	Valid
Description:	An external or internal diagnostic tool needs access to the fault memory to get or change information about the fault status. An interface between diagnostic communication management and diagnostic event management is required.
Rationale:	The DCM and the DEM are separated modules with the necessity to interact. Therefore an interface is necessary.
Use Case:	A diagnostic test tool needs to read or clear the fault memory with the corresponding diagnostic services, e.g. “ReadDTCInformation”, “ClearDiagnosticInformation”
Dependencies:	[SRS_Diag_04002] Diagnostic event (error) management
Supporting Material:	--

⌋(RS_BRF_01440, RS_BRF_02144)

4.3.24.2 [SRS_Diag_04011] The DCM shall provide diagnostic state information for AUTOSAR Software Component via RTE

[

Type:	Valid
Description:	The Software modules above the RTE need to know about the actual session and security state, because it is not predictable if the information's lead to a different functional diagnostic behavior.
Rationale:	Functional requirement
Use Case:	With the diagnostic session which the garage is using, it is allowed to switch between different sets of parameters. With an enhanced diagnostic session which could be used in development and a corresponding security level, it is allowed to change the data within the set of parameters.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.3.24.3 [SRS_Diag_04003] The interface of the DCM to PDU Router (CAN/LIN; FlexRay; MOST) shall be network independent

[

Type:	Valid
Description:	All network (CAN, LIN, FlexRay, MOST) dependent parts shall be done outside the DCM module. That means the module PDU Router shall provide a network independent interface.
Rationale:	The DCM describes only the services for communication and the behavior of network is out of scope. Highest granularity and best option to adapt upcoming networks.
Use Case:	DCM has to be network independent. So, the interface to the Transport Protocol shall be network independent.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_01720)

4.3.24.4 [SRS_Diag_04147] The DCM shall communicate with the PDU Router to receive and send diagnostic data

[

Type:	Valid
Description:	The DCM shall communicate with the PDU Router to receive and send diagnostic data.
Rationale:	Ensure diagnostic communication.
Use Case:	Support of various transport protocols (ISO-15765-2,...).
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_01720)

4.4 Function Inhibition Manager (FIM)

The specification of software requirements of the function inhibition manager is not a part of this specification. For detailes please refer to the AUTOSAR_FIM_SRS.

4.5 Defaut Error Tracer (DET)

4.5.1 [SRS_Diag_04090] A configurable list of error report receivers shall be [provided

Type:	Valid
Description:	The Default Error Tracer shall support a configurable list of functions for fan-out of received error reports. This list can be empty.
Rationale:	This implements the debugging concept in R4.0 (DocumentId 298).
Use Case:	- Even development errors shall be captured by the Log and Trace functionality - Error Handling shall be enabled to react on development errors
Dependencies:	--
Supporting Material:	--

](RS_BRF_02168)

4.5.2 [SRS_Diag_04086] Report errors shall contain a dedicated set of information

[

Type:	Valid
Description:	Error reports, which the Default Error Tracer receives, shall consist of the ID of the reporting module, the ID of reporting instance, the ID of the API service in which the error has been detected and the error id it self.
Rationale:	For optimal support of the error tracing some tracing information is necessary.
Use Case:	During software development phase a BSW module has been called using wrong parameters. Due to communication of some tracing information the location of the error source will be supported.
Dependencies:	--
Supporting Material:	--

](RS_BRF_02168)

4.5.3 [SRS_Diag_04087] The Default Error Tracer shall provide a development error report reception service

[

Type:	Valid
Description:	The Default Error Tracer shall be accessible by SW-C's to report development error.
Rationale:	It shall be possible to perform error tracing during development of SW-C's.
Use Case:	During software development phase a SW-C has received an unexpected response by a BSW module. By generating a development error and reporting it to the DET, configuration errors can be detected.
Dependencies:	--
Supporting Material:	--

](RS_BRF_02168)

4.5.4 [SRS_Diag_04089] Fan-out of received error reports

[

Type:	Valid
Description:	The Default Error Tracer shall forward each received error report by calling each element of a configurable list of functions.
Rationale:	This implements the debugging concept in R4.0 (DocumentId 298)
Use Case:	- Even development errors shall be captured by the Log and Trace functionality - Error Handling shall be enabled to react on development errors
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02240)

4.5.5 [SRS_Diag_04085] The Default Error Tracer shall provide an interface to receive error reports

[

Type:	Valid
Description:	The Default Error Tracer shall provide an interface to get a development error report.
Rationale:	An interface will be needed to enable handling of development errors
Use Case:	During software development phase a BSW module has been called using wrong parameters. By generating a development error and reporting it to the DET, configuration errors can be detected.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_01056)

4.5.6 [SRS_Diag_04101] The DET module shall forward its trace events to the DLT

[

Type:	Valid
Description:	The DET receives trace events from errors from the BSW and SWC during debugging time. If a DLT module exists, these events should be forwarded to the DLT to collect logs and traces only in one instance.
Rationale:	To have an overview of all log, trace and error messages and to set all of them in the correct context, it is important to have all these messages and events in one list (context). Also it is not practicable to use more than one mechanism to report errors, logs and traces to a debugging interface. So all these sources should be routed to the DLT.
Use Case:	• in a debugging scenario, an SWC or BSW Module uses the DET interface to trace an error • this error is forwarded by the DET to the DLT • the DLT turns these events in the DLT format and sends it over the debugging interface, together with all the other logs and traces
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

4.5.7 [SRS_Diag_04143] The Default Error Tracer shall provide an interface to receive runtime error reports

⌈

Type:	Valid
Description:	The Default Error Tracer shall provide an interface to get a runtime error report, issued by BSW modules. The Default Error Tracer returns to the caller in order to allow continuation of intended program flow.
Rationale:	An interface will be needed to enable handling of runtime errors, caused by seldom occurring systematic faults. The caller will handle the error and continue appropriate in a deterministic manner.
Use Case:	CANNM_E_NET_START_IND: Reception of NM PDUs in Bus-Sleep Mode
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440, RS_BRF_01056)

4.5.8 [SRS_Diag_04144] The Default Error Tracer shall provide an interface to receive transient fault reports

⌈

Type:	Valid
Description:	The Default Error Tracer shall provide an interface to get a transient fault report, issued by BSW modules. The Default Error Tracer returns to the caller in order to allow continuation of intended program flow.
Rationale:	An interface will be needed to enable handling of transient faults, caused by seldom occurring transient hardware faults.
Use Case:	• CAN controller goes offline due to bit-flip in its control register. • Peripheral action lasts accidentally longer than expected (and specified)
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440, RS_BRF_01056)

4.5.9 [SRS_Diag_04145] The Default Error Tracer shall forward received runtime error reports to configured integrator code

⌈

Type:	Valid
Description:	The Default Error Tracer shall propagate all received runtime error reports using configurable callout. The received callout return value shall be returned to the reporter of the runtime error. If no callout has been configured, a default return value shall be provided. The Default Error Tracer returns to the caller in order to allow continuation of intended program flow.
Rationale:	Integrator shall be able to recognize runtime errors and to handle in an appropriate manner.
Use Case:	CANNM_E_NET_START_IND: Reception of NM PDUs in Bus-Sleep Mode
Dependencies:	--
Supporting Material:	--

⌋(RS_BRF_01440, RS_BRF_01056)

4.5.10 [SRS_Diag_04146] The Default Error Tracer shall forward received transient fault reports to configured integrator code

⌈

Type:	Valid
Description:	The Default Error Tracer shall propagate all received transient fault report

	using configurable callout. The received callout return value shall be returned to the reporter of the transient fault. If no callout has been configured, a default return value shall be provided. The Default Error Tracer returns to the caller in order to allow continuation of intended program flow.
Rationale:	Integrator shall be able to recognize transient faults and to handle in an appropriate manner and to advice the reporter.
Use Case:	• CAN controller goes offline due to bit-flip in its control register. Integrator decides that reporting CAN driver shall re-initialize the CAN controller. • CAN controller goes offline due to bit-flip in its control register. Integrator decides that reporting CAN driver shall treat offline state of CAN controller as intended.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440, RS_BRF_01056)

4.6 Configuration

4.6.1 [SRS_Diag_04059] The DCM and DEM shall support the configuration of timing parameters

[

Type:	Valid
Description:	Every physical layer requires specific timing parameter values therefore it is necessary to include the ability to configure the timing constrains depending on the used network. The timing parameters are set to default values when a communication starts and shall be changeable at runtime.
Rationale:	Usability with different networks.
Use Case:	The diagnostic communication can be done at different networks (e.g. CAN/LIN/FlexRay).
Dependencies:	[SRS_Diag_04015] Provision of timing handling according to ISO15765-3
Supporting Material:	--

](RS_BRF_01440, RS_BRF_02200)

4.6.2 [SRS_Diag_04064] The DEM shall support buffers of scalable sizes for the storage of the events, status information and environmental data

[

Type:	Valid
Description:	a) For the internal administration the DEM needs an Event buffer which shall be configurable depending on the number of the possible events in the system i.e. related to all SW components which are assigned to the DEM b) The fault storage [event buffer] shall provide enough space to store all high priority failures.
Rationale:	Processor resource constraints
Use Case:	In case of large Systems with many events a selection of Events shall take place to fulfill NVRAM / RAM constraints of smaller processors.
Dependencies:	--
Supporting Material:	--

](RS_BRF_01440)

5 References

5.1 Deliverables of AUTOSAR

[1] General Requirements of Basic Software Modules
AUTOSAR_SRS_BSWGeneral.pdf

[2] Specification of the Virtual Functional Bus
AUTOSAR_EXP_VFB.pdf

[3] Software Standardization Template
AUTOSAR_TPS_StandardizationTemplate.pdf

5.2 Related standards and norms

5.2.1 ITEA-EAST

[4] D1.5-General Architecture; ITEA/EAST-EEA, Version 1.0; chapter 3, page 72 et seq.

[5] D2.1-Embedded Basic Software Structure Requirements; ITEA/EAST-EEA, Version 1.0 or higher

[6] D2.2-Description of existing solutions; ITEA/EAST-EEA, Version 1.0 or higher.

5.2.2 ISO

[7] ISO 14229-1 Unified diagnostic services (UDS) – Part 1: Specification and Requirements (v.2013)

[8] ISO 15031-5 Communication between vehicle and external equipment for emissions-related diagnostics – Part 5: Emissions-related diagnostic services (2005-01-13)

[9] ISO 15765-3 Diagnostics on controller area network (CAN) – Part 3: Implementation of unified diagnostic services (UDS on CAN) (2004-10-06)

[10] ISO 15765-4 Diagnostics on controller area network (CAN) – Part 4: Requirements for emissions-related systems (2005 01-04)

5.3 Requirement change history

5.3.1 Changes to Release 3.1

Removed BSW Item	*Rationale*
BSW04017	Obsolete because the DCM design changed
BSW04108	Already covered by SRS_Diag_04097
BSW04088	DET functionality not needed by any concept

Replaced BSW Item	*Rationale*
none	

Changed BSW Item	*Rationale*
SRS_Diag_04058	Improve description
SRS_Diag_04024	Improve description
SRS_Diag_04066	Improve description
SRS_Diag_04068	Improve description

Added BSW Item	*Rationale*
SRS_Diag_04085	Requirements of Default Error tracer (DET)
SRS_Diag_04086	Requirements of Default Error tracer (DET)
SRS_Diag_04087	Requirements of Default Error tracer (DET)
BSW04088	Requirements of Default Error tracer (DET)
SRS_Diag_04089	Requirements of Default Error tracer (DET)
SRS_Diag_04090	Requirements of Default Error tracer (DET)
SRS_Diag_04091	Notification about valid freeze frame data (RS_BRF_00231)
SRS_Diag_04092	Control of event handling (RS_BRF_00230)
SRS_Diag_04093	Overflow indication (RS_BRF_00233)
SRS_Diag_04095	DEM behaviour concept (RS_BRF_00230)
SRS_Diag_04096	DEM behaviour concept (RS_BRF_00230)
SRS_Diag_04097	Decentralized modular diagnostic configuration of SW-Cs (RS_BRF_00229)
SRS_Diag_04098	Bootloader interaction (RS_BRF_00034)
SRS_Diag_04100	DCM Support for diagnostic log & trace (DLT), RS_BRF_00295
SRS_Diag_04101	DET Support for diagnostic log & trace (DLT) RS_BRF_00295
SRS_Diag_04102	DEM behaviour concept (RS_BRF_00230)
SRS_Diag_04104	DEM behaviour concept (RS_BRF_00230)
SRS_Diag_04105	DEM behaviour concept (RS_BRF_00230)
SRS_Diag_04106	DEM behaviour concept (RS_BRF_00230) - removed
SRS_Diag_04107	Savety concept (RS_BRF_00129)
SRS_Diag_04109	Retrieving number of event memory entries
SRS_Diag_04110	Requirements on Diagnostic
SRS_Diag_04111	Requirements on Diagnostic
SRS_Diag_04112	Requirements on Diagnostic
SRS_Diag_04113	Requirements on Diagnostic
SRS_Diag_04115	Requirement for DEM
SRS_Diag_04116	Requirement for DEM
SRS_Diag_04117	Requirement for DEM
SRS_Diag_04118	Requirement for DEM

SRS_Diag_04119	Requirement for DCM
SRS_Diag_04120	Requirement for DCM
SRS_Diag_04121	Requirement for DCM
SRS_Diag_04122	Requirement for DEM
SRS_Diag_04123	Requirement for DEM
SRS_Diag_04124	Requirement for DEM
SRS_Diag_04125	Requirement for DEM
SRS_Diag_04126	Requirement for DEM
SRS_Diag_04127	Requirement for DEM
SRS_Diag_04128	Requirement for DEM
SRS_Diag_04129	Requirement for DEM
SRS_Diag_04130	Requirement for DEM
SRS_Diag_04131	Requirement for DEM
SRS_Diag_04133	Requirement for DEM
SRS_Diag_04134	Requirement for DEM
SRS_Diag_04135	Requirement for DCM
SRS_Diag_04136	Requirement for DEM
SRS_Diag_04137	Requirement for DEM
SRS_Diag_04138	Requirement for DCM
SRS_Diag_04139	Requirement for DCM and DEM
SRS_Diag_04140	Requirement for DEM
SRS_Diag_04141	Requirement for DCM and DEM
SRS_Diag_04142	Requirement for DEM
SRS_Diag_04143	Requirement for DLT
SRS_Diag_04144	Requirement for DLT
SRS_Diag_04145	Requirement for DLT
SRS_Diag_04146	Requirement for DLT
SRS_Diag_04147	Requirement for DCM